Periods of the discretized Arnold's Cat Mapping and its extension to n-dimensions

Joe Nance
nance2uiuc@gmail.com
Department of Mathematics
University of Illinois at Urbana-Champaign

June 23, 2011

Abstract

A discrete dynamical system known as Arnold's Discrete Cat Map is given by

$$(x_{t+1}, y_{t+1}) = (x_t + y_t, x_t + 2y_t) \ mod \ N$$

acting on a two-dimensional square coordinate grid of size $N \times N$. The defining characteristic of this map is that it has the property that when the $N \times N$ grid is a picture whose pixels are assigned (x, y) coordinates, the map scrambles the picture with each iteration. After a finite number of iterations, the picture is restored to its original shape and order. The number of iterations needed to restore the image M, has a mysterious dependence on N. This period, as we will find out, is directly related to the divisibility of the Fibonacci numbers. We will exploit this property to show that for any N, an image is not dense in itself. In the second half of the paper, we build on the work of Chen, Mao, and Chui to extend the DCM to three dimensions. Finally, we define the generalized n dimensional DCM by introducing the idea of a "matrix union".

1 The nature of the 2D DCM

Arnold's Cat Mapping is a chaotic mapping on the two dimensional torus given by

$$A(x, y) = (x + y, x + 2y) \ mod \ 1$$

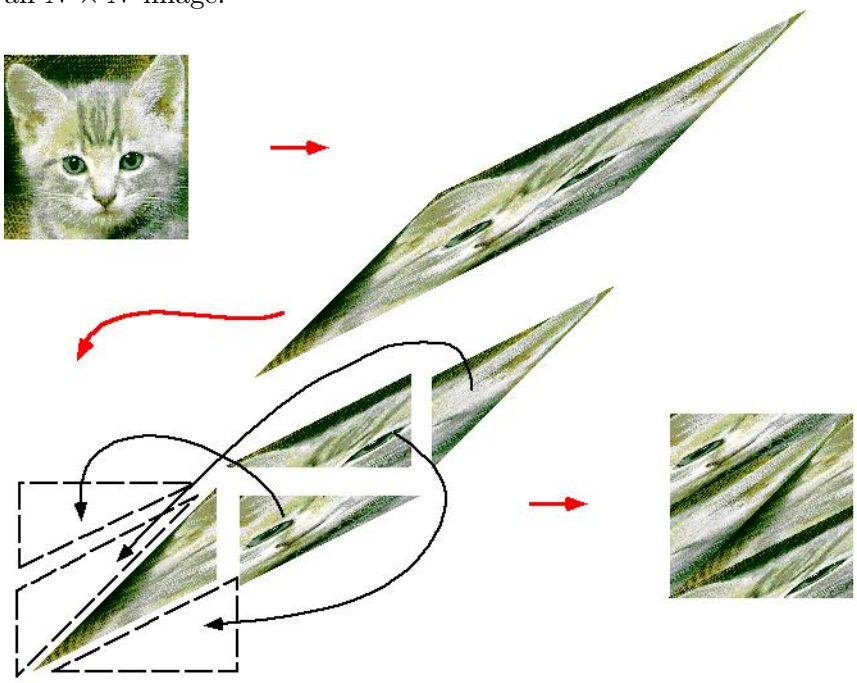
but for our purposes, we will use the discretized version

$$(x_{t+1}, y_{t+1}) = (x_t + y_t, x_t + 2y_t) \ mod \ N$$

where N is the size of the discrete grid on which the map acts. The 2D DCM can be written equivalently in matrix form as

$$\begin{pmatrix} x_{t+1} \\ y_{t+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x_t \\ y_t \end{pmatrix} \ mod \ N$$

Figure 1: Geometrically, this is what a single iteration of the DCM does to an $N \times N$ image.



Example 1.1. Consider an arbitrary 3×3 image given by $\begin{bmatrix} A & B & C \\ D & E & F \\ G & H & I \end{bmatrix}$.

The (x, y)-coordinates of the pixels in this image are $\begin{bmatrix} (0,2) & (1,2) & (2,2) \\ (0,1) & (1,1) & (2,1) \\ (0,0) & (1,0) & (2,0) \end{bmatrix}$ mod 3.

Let's look at the orbit of an arbitrary pixel under the DCM,

$$(1,1) \to (2,0) \to (2,2) \to (1,0) \to (1,1).$$

The orbit of the entire image looks like

$$\begin{bmatrix} A & B & C \\ D & E & F \\ G & H & I \end{bmatrix} \to \begin{bmatrix} B & D & I \\ F & H & A \\ G & C & E \end{bmatrix} \to \begin{bmatrix} D & F & E \\ A & C & B \\ G & I & H \end{bmatrix} \to \begin{bmatrix} F & A & H \\ B & I & D \\ G & E & C \end{bmatrix} \to \begin{bmatrix} A & B & C \\ D & E & F \\ G & H & I \end{bmatrix}$$

So a 3×3 image has period $M = 4$ since four iterations of the cat map were needed to return the image to its original state.

pixel dimension of image ($N \times N$)	iterations to restore image (period)
300×300	300
257×257	258
183×183	60
157×157	157
150×150	300
147×147	56
124×124	15
100×100	150

Table 1: Notice, there is not an apparent correlation between the size of an image and its period.

Dyson and Falk give some relationships and bounds on the period of an image of size N:

$$M \begin{array}{l} = 3N \text{ for } N = 2(5^s)\ ; s \in \mathbb{N} \\ = 2N \text{ for } N = 5^s \text{ or } 6(5^s)\ ; s \in \mathbb{N} \\ \leq \frac{12N}{7} \text{ for other } N \end{array}$$

2 An image is not dense in itself

As in Example 1.1, consider the orbit of a single pixel as it jumps around an image with each iteration. An interesting question to ask is, "Does there exist N such that every pixel visits every other pixel at least once?" or perhaps more formally, "Does there exist N such that an image is dense in itself?"

To answer this question, it will be convenient to use the matrix

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \text{ where } A^2 =: A_2 = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$$

and define the Fibonacci sequence as $u_0 = 0,\ u_1 = 1,\ u_2 = 1,\ u_3 = 2, u_4 = 3, ..., [u_{t+2} = u_{t+1} + u_t]$. Then, the matrix for the t^{th} iteration of the DCM is given by

$$A^{2t} = \begin{pmatrix} u_{2t-1} & u_{2t} \\ u_{2t} & u_{2t+1} \end{pmatrix}$$

For a given N, the period M of the DCM is the smallest positive integer t such that $u_{2t} \equiv 0\ mod\ N$ and $u_{2t-1} \equiv 1\ mod\ N$ which implies that $u_{2t+1} \equiv u_{2t+2} \equiv 1\ mod\ N$. Thus, the period M of the DCM for a given image size N is strongly related to the divisibility of the Fibonacci numbers. Dyson and Falk give the following theorem and proof in [2]. The fact that an image is not dense in itself follows as a corollary.

Theorem 2.1. *For an image of size $N \times N$ where $N \geq 3$, the period of this image, $M \leq \frac{N^2}{2}$.*

Before we can prove this theorem, we will prove three short lemmas.

Definition 2.2. Define ϕ_i as the least non-negative residue of u_i, the i^{th} Fibonacci number *mod* N. That is, $u_i \equiv \phi_i \bmod N$.

Consider the sequence of ordered pairs $\langle\phi_1, \phi_2\rangle, \langle\phi_2, \phi_3\rangle, ..., \langle\phi_i, \phi_{i+1}\rangle, ...$ There are at most N^2 distinct pairs. Any set of $N^2 + 1$ pairs contains some equal ones among them.

Lemma 2.3. *The first pair that repeats in the above sequence is* $\langle 1, 1\rangle$.

Proof. Assume the opposite: that the first repeated pair is $\langle\phi_k, \phi_{k+1}\rangle$, where $k > 1$. So let's find a pair $\langle\phi_r, \phi_{r+1}\rangle$ where $(r > k)$ in the sequence such that $\phi_k = \phi_r, \phi_{k+1} = \phi_{r+1}$. From the definition of the Fibonacci numbers,

$$\phi_{r-1} = \phi_{r+1} - \phi_r$$

$$\phi_{k-1} = \phi_{k+1} - \phi_k$$

so $\phi_{r-1} = \phi_{k-1}$ and we have that $\langle\phi_{r-1}, \phi_r\rangle = \langle\phi_{k-1}, \phi_k\rangle$. But $\langle\phi_{k-1}, \phi_k\rangle$ occurs earlier in the sequence than $\langle\phi_k, \phi_{k-1}\rangle$; therefore $\langle\phi_k, \phi_{k-1}\rangle$ is not the first pair that repeats itself. So the supposition $k > 1$ is wrong so $k = 1$. This proves the lemma. □

Lemma 2.4. *For any positive integer* N*, at least one number divisible by* N *can be found among the first* N^2 *Fibonacci numbers.*

Proof. From the previous lemma, $\langle 1, 1\rangle$ is the first pair that repeats itself. So $\langle\phi_t, \phi_{t+1}\rangle = \langle 1, 1\rangle$ for some integer t such that $1 < t \leq N^2 + 1$. Thus

$$\phi_t \equiv 1 \bmod N$$

and

$$\phi_{t+1} \equiv 1 \bmod N.$$

But

$$u_{t-1} = u_{t+1} - u_t$$

therefore,

$$\phi_{t-1} \equiv 0 \bmod N$$

This proves the lemma. □

Lemma 2.5. *For $N > 2$ if $u_t \equiv 0$ mod N and $u_{t+1} \equiv 1$ mod N, then t must be even.*

Proof. The lemma is equivalent to the statement that for $N > 2$, if $A^t \equiv 1 \bmod N$, then t is even. But $det(A) = -1$, so $det(A^t) = (det\ A)^t = (-1)^t \equiv 1 \bmod N$. Hence t must be even. This proves the lemma. □

Theorem 2.6. *The period, M of the DCM satisfies $M \leq \frac{N^2}{2}$.*

Proof. From the first and second lemmas, the second occurrence of the pattern $0, 1, 1$ in the sequence $\phi_0, \phi_1, ..., \phi_t, \phi_{t+1}, ...$ happens for $\phi_{j-1}, \phi_j, \phi_{j+1}$, where $0 < j - 1 \leq N^2$. From the third lemma, $j - 1$ must be even. From the definition of the period, we have that $2M = j - 1$. This proves the theorem. □

Corollary 2.7. An image is not dense in itself.

Proof. Suppose there exists an N such that an $N \times N$ image was dense in itself. For this to be true, it would have to be the case that the period of the image equals $N^2 - 1$ since there are N^2 pixels and without any iterations, the pixel occupies itself. But from the theorem, an arbitrary pixel in an $N \times N$ image has a period at most of half the total number of pixels in the image; a contradiction. Therefore, the number of unique places that an arbitrary pixel occupies in one full cycle is never more than half of the number of possible places. Since the choice of pixel is arbitrary, this theorem holds for the whole image. So an image is not dense in itself under the discrete cat map. This proves the corollary. □

3 Higher dimensional analogs

What would a three dimensional analog to the $2D$ DCM look like? Certainly, the mapping would have to act on an $N \times N \times N$ cube. An N-cube would have to posses a finite period, like its $2D$ cousin. The mapping would also have to posses the area-preserving and mixing dynamics of the $2D$ DCM. A plausible

way to obtain an explicit form for the $3D$ DCM would be to compose three mappings. Each mapping would fix one coordinate of x, y, z-space and have the lower dimensional DCM act on the remaining two coordinates. This way, after composition of the three "basis" maps, the entire $N \times N \times N$ cube has been mapped in the way of the cat.

We have

$$\mathbf{A_2} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}.$$

Fixing x, we obtain the first of three "basis" maps,

$$a_3^1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 2 \end{pmatrix}.$$

Fixing y, we obtain the second basis map,

$$a_3^2 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 2 \end{pmatrix}.$$

Fixing z, the third basis map is

$$a_3^3 = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Composition of linear functions dictates that we multiply their respective matrix representations,

$$\mathbf{A_3} = a_3^1 a_3^2 a_3^3 = \begin{pmatrix} 1 & 1 & 1 \\ 2 & 3 & 2 \\ 3 & 4 & 4 \end{pmatrix}.$$

This is the matrix for the three dimensional discrete cat map.

3.1 The concept of "matrix union"

The systematic extrapolation of the $2D$ DCM to three dimensions can be generalized for an arbitrary positive integer dimension. We just need to

introduce a bookkeeping device to formalize the action of fixing a coordinate in a basis map.

Definition 3.1. $\{F_n^i\}$ is the set of "$n \times n$ i-frames",

$$F_n^i = \begin{pmatrix} & & & 0 & & & \\ & & & \vdots & & & \\ & & & 0 & & & \\ 0 & \cdots & 0 & d_i & 0 & \cdots & 0 \\ & & & 0 & & & \\ & & & \vdots & & & \\ & & & 0 & & & \end{pmatrix}$$

where $d_i = 1$ is the i^{th} diagonal and the i^{th} row and column except for the entry $[d_i]$ consist entirely of 0's.

Example 3.2.

$$F_3^2 = \begin{pmatrix} & 0 & \\ 0 & 1 & 0 \\ & 0 & \end{pmatrix}, \; F_3^1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & & \\ 0 & & \end{pmatrix}$$

Definition 3.3. The matrix union $\mho$ is a binary function $\mho : \mathbf{A_n} \times F_{n+1}^i \to a_{n+1}^i$ which takes an n dimensional DCM matrix $\mathbf{A_n}$ and inserts it into an $n+1$ dimensional i-frame. The output is an $n+1$ dimensional basis map a_{n+1}^i which fixes the i^{th} coordinate of the n dimensional DCM.

Definition 3.4. A basis map a_{n+1}^i is an element of the "union basis" of $\mathbf{A_n}$, $\{a_{n+1}^i\} = \{\mho(\mathbf{A_n}, F_{n+1}^i)\}_{i=1}^{n+1}$. This matrix fixes the i^{th} coordinate of the n dimensional DCM.

Example 3.5.

$$\mho(\mathbf{A_2}, F_3^1) = a_3^1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 2 \end{pmatrix}, \; \mho(\mathbf{A_3}, F_4^3) = a_4^3 = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 2 & 3 & 0 & 2 \\ 0 & 0 & 1 & 0 \\ 3 & 4 & 0 & 4 \end{pmatrix}$$

This new machinery allows for a concise iterative expression for the matrix for the n dimensional DCM,

$$\mathbf{A_{n+1}} = \prod_{i=1}^{n+1} \mho(\mathbf{A_n}, F_{n+1}^i); \; n \geq 2 \tag{1}$$

Example 3.6. Generate the matrix for the $4D$ DCM. Using (1), we have

$$a_4^1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 2 & 3 & 2 \\ 0 & 3 & 4 & 4 \end{pmatrix} a_4^2 = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 2 & 0 & 3 & 2 \\ 3 & 0 & 4 & 4 \end{pmatrix} a_4^3 = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 2 & 3 & 0 & 2 \\ 0 & 0 & 1 & 0 \\ 3 & 4 & 0 & 4 \end{pmatrix} a_4^4 = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 2 & 3 & 2 & 0 \\ 3 & 4 & 4 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

And so

$$\mathbf{A_4} = a_4^1 a_4^2 a_4^3 a_4^4 = \begin{pmatrix} 17 & 23 & 18 & 5 \\ 110 & 149 & 117 & 31 \\ 257 & 348 & 274 & 72 \\ 432 & 585 & 460 & 122 \end{pmatrix}.$$

3.2 Dynamical properties of higher dimensional cat maps

We now focus our attention on the general cat map whose t^{th} iteration is given by $\vec{x}_t = \mathbf{A_n}^t \vec{x}_0$, where $\mathbf{A_n}$ is the matrix derived in the preceding section. In this mapping, we allow $\vec{x}_0$ to be continuous. Unlike the DCM, this map allows for points with irrational coordinates. This way, the mapping has chaotic orbits.

Definition 3.7. (Alligood, Saur, and Yorke Def. 5.2) Let $\mathbf{f}$ be a map of $\mathbb{R}^m$, $m \geq 1$, and let $\{\mathbf{v}_0, \mathbf{v}_1, \mathbf{v}_2, ...\}$ be a bounded orbit of $\mathbf{f}$. This orbit is chaotic if: it is not asymptotically periodic, $\mathbf{f}$ has no eigenvalue equal to 1, and at least one eigenvalue is greater than 1 in absolute value.

For an orbit of the general cat map, an argument using folliations of the torus (which is beyond the scope of this paper) can be used to show that if a point has irrational coordinates, then its orbit is not asymptotically periodic. For the second two conditions, it boils down to finding the characteristic polynomial of $\mathbf{A_n}$. If $(x-1) \nmid \chi_{\mathbf{A_n}}(\lambda)$ and at least one root of $\chi_{\mathbf{A_n}}(\lambda)$ is greater than 1 in absolute value, then any orbit of the general cat map whose coordinates are irrational is chaotic. Characteristic polynomials are given for the first few cases of the n dimensional general cat map below:

$$\chi_{\mathbf{A_2}}(\lambda) = \lambda^2 - 3\lambda + 1$$
$$\chi_{\mathbf{A_3}}(\lambda) = -\lambda^3 + 8\lambda^2 - 6\lambda + 1$$
$$\chi_{\mathbf{A_4}}(\lambda) = \lambda^4 - 562\lambda^3 + 410\lambda^2 - 66\lambda + 1.$$

Approximate forms for eigenvalues are given respectively as:

$$0.381966,\ 2.61803$$
$$0.243019,\ 0.572771,\ 7.18421$$
$$0.0168808,\ 0.209427,\ 0.50397,\ 561.27.$$

As you can see, so far there are not any eigenvalues equal to 1 and at least one eigenvalue is larger than 1 in absolute value in each case. These eigenvalues can be loosely interpreted as the amount of stretching on a per iteration basis of the nearby orbits under the map, where the largest value dominates the stretching behavior. In a sense, these numbers measure how chaotic a system is.

I conjecture, but am not able to prove, that as the dimension of the generalized cat map increases, the dominant eigenvalue of the map increases. Hence, larger dimensional analogs are more chaotic than their lower dimensional counterparts. Since we have an iterative way using the matrix union to generate higher dimensional matrices for an arbitrary cat map which factors as a product of easily understood basis maps, I propose that in order to prove or disprove this, one would need to develop some way of studying the interaction of characteristic polynomials under the action of multiplying their corresponding matrices. This way, one may be able to establish a bijection between the natural numbers and absolute values of eigenvalues of cat maps of increasing dimension.

References

[1] Peterson, Gabriel. "Arnold's Cat Map." College of the Redwoods. Ed. David Mills. N.p., Sept. 1997. Web. 3 Mar. 2011.

[2] F. Dyson and H. Falk. "Period of a Discrete Cat Mapping." *The American Mathematical Monthly*99.7 Aug. (1992): 603-14.

[3] Chen, Mao, and Chui. "A symmetric image encryption scheme based on 3D chaotic cat maps." *Chaos, Solitons, and Fractals*1.21 (2004): 749-61.

[4] Alligood, Kathleen T., Tim D. Saur, and James A. Yorke. Chaos: An Introduction to Dynamical Systems. New York: Springer, 1996.